CLAIMS

1. A method of regulating access to at least one service provided by at least one service provider, wherein a service authoriser:

- generates for each of multiple service time periods a different respective data set comprising private data and related public data; and
- determines whether a party is entitled to receive a said service for a particular said time period and, if so, provides that party with a decryption key for accessing the service during said particular time period, the decryption key being generated by the authoriser in dependence on both an arbitrary encryption key string associated with the service, and the private data of the data set for said particular time period.

2. A method according to claim 1, wherein a said service provider provides said party with encrypted data which the party is required to decrypt to receive the service for a current said time period, the encrypted data being data encrypted based on said encryption key string and the public data of the data set for said current time period, and the party only being able to decrypt the encrypted data using said decryption key provided by the authoriser where the said particular time period is said current time period.

3. A method according to claim 2, wherein the data that is encrypted by the service provider is arbitrary data, said party being required to decrypt and return this data as evidence of its entitlement to receive the service for the current time period before the service provider provides said service to the party.

4. A method according to claim 2, wherein the data that is encrypted by the service provider is a data component of the service.

5. A method according to claim 4, wherein the data component comprises at least one of software and digital media content.

6. A method according to claim 1, wherein the encryption key string is formed using at least an identifier of said service.

7. A method according to claim 6, wherein the service identifier is generated by said party and provided by it both to the authoriser to obtain the decryption key for enabling the party to receive the service during said particular time period, and to the service provider concerned.

8. A method according to claim 7, wherein the service provider maps the service identifier to the most suitable one of multiple services it can provide in order to determine the service required by said party.

9. A method according to claim 6, wherein the service identifier is generated by one of the authoriser and the service provider concerned and made available both to the other of the service provider and authoriser, and to said party.

10. A method according to claim 1, wherein plural said data sets are generated in advance of the time periods to which they relate and the public data of these data sets are made available in advance of those time periods to at least one of said party and said at least one service provider.

11. A method according to claim 1, wherein the time for which said service is available is divided into time slots, each said time period for which a respective said data set is generated corresponding to a respective one of said time slots.

12. A method according to claim 1, wherein the time for which said service is available is divided into time slots, at least one of said time periods for which a respective said data set is generated corresponding to a combination of multiple said time slots.

13. A method according to claim 1, wherein the time for which said service is available is divided into time slots, and wherein for a group of successive time slots, each time slot and each of every possible time-ordered combination of at least two adjacent time slots constitutes a respective said time period for which a corresponding data set is generated by the authoriser, the authoriser providing a single decryption key to said party upon

determining that the party is entitled to receive said service for any time slot or time-ordered combination of time slots within said group.

14. A method according to claim 1, wherein at least one of the start and finish of a said time period is determined by the occurrence of a non-clock event.

15. A method according to claim 1, wherein the decryption key provided to said party in respect of a time period for which it is entitled to receive said service, is securely stored in trusted platform equipment of said party such that the decryption key is not accessible in cleartext form to the party but is usable to decrypt said encrypted data in the trusted platform.

16. A method according to claim 1, wherein the authoriser operates to determine the entitlement of said party to any of multiple services for any of said multiple time periods, and to provide the party with at least one decryption key appropriate for the or each service and the or each time period for which the party has been determined as entitled, the decryption keys for each of said multiple services in the same time period being different from each other.

17. A method according to claim 16, wherein the authoriser uses the private data of the same data set for each service during the same time period when generating the decryption key to be provided to said party, the encryption key strings used for each of said multiple services being different from each other.

18. A method according to claim 16, wherein the authoriser generates a respective data set for each combination of service and time period, the authoriser using the private data of the data set for the appropriate service and time period when generating the decryption key to be provided to said party.

19. A computing entity for regulating access to at least one service provided by at least one service provider, the computing entity comprising:

- first means for generating for each of multiple service time periods a different respective data set comprising private data and related public data;
- second means for determining whether a party is entitled to receive a said service for a particular said time period;
- third means for providing a party that the second means has determined is entitled to receive the service, with a decryption key for accessing the service during said particular time period, the third means including key-generating means for generating the decryption key in dependence on both an arbitrary encryption key associated wit the service, and the private data of the data set for said particular time period.

20. A computing entity according to claim 19, wherein the encryption key string is formed using at least an identifier of said service.

21. A computing entity according to claim 20, wherein the computing entity is arranged to receive said service identifier from said party.

22. A computing entity according to claim 20, wherein the computing entity is arranged to generate the service identifier and to make it available to the service provider concerned and said party.

23. A computing entity according to claim 19, wherein the computing entity is arranged to use said first means to generate plural said data sets in advance of the time periods to which they relate, the computing entity being further arranged to make the public data of these data sets available in advance of those time periods to at least one of said party and the service provider concerned.

24. A computing entity according to claim 19, wherein the time for which said service is available is divided into time slots, each said time period for which a respective said data set is arranged to be generated by said first means corresponding to a respective one of said time slots.

25. A computing entity according to claim 19, wherein the time for which said service is available is divided into time slots, at least one of said time periods for which a respective said data set is arranged to be generated by said first means corresponding to a combination of multiple said time slots.

26. A computing entity according to claim 19, wherein the time for which said service is available is divided into time slots, and wherein for a group of successive time slots, each time slot and each of every possible time-ordered combination of at least two adjacent time slots constitutes a respective said time period for which said first means is arranged to generate a corresponding data set, the third means being arranged to provide a single decryption key to said party upon the second means determining that the party is entitled to receive said service for any time slot or time-ordered combination of time slots within said group.

27. A computing entity according to claim 19, wherein the first means includes means for determining the occurrence of a non-clock event and for using this occurrence to start or finish of a said time period.

28. A computing entity according to claim 19, wherein the second means is arranged to determine the entitlement of said party to any of multiple services for any of said multiple time periods, the third means being arranged to provide said party with at least one decryption key appropriate for the or each service and the or each time period for which the party has been determined as entitled, the decryption keys for each of said multiple services in the same time period being different from each other.

29. A computing entity according to claim 28, wherein the key-generating means is arranged to use the private data of same data set for each service during the same time period when generating the decryption key to be provided to said party, the encryption key strings used for each of said multiple services being different from each other.

30. A computing entity according to claim 28, wherein the first means is arranged to generate a respective data set for each combination of service and time period, the key-

generating means being arranged to use the private data of the data set for the appropriate service and time period when generating the decryption key to be provided to said party.

31. A system for regulating access to a service provided by a service provider, the system comprising:

- a first computer entity for authorising access to said service, comprising:
  - first means for generating for each of multiple service time periods a different respective data set comprising private data and related public data;
  - second means for determining whether the party is entitled to receive the service for a particular said time period;
  - third means for providing a party that the second means has determined is entitled to receive the service, with a decryption key for accessing the service during said particular time period, the third means including key-generating means for generating the decryption key in dependence on both an arbitrary encryption key associated with the service, and the private data of the data set for said particular time period;
- a second computer entity, associated with the service provider, and arranged to provide said party with encrypted data which the party is required to decrypt to receive the service for a current said time period, the second computer entity being arranged to form said encrypted data by encrypting data based on said encryption key string and the public data of the data set for said current time period; and
- a third computer entity, associated with said party, and arranged to use the decryption key provided by the first computer entity to decrypt the encrypted data provided by the second computer entity, the third computer entity only being able to decrypt the encrypted data using said decryption key where the said particular time period is said current time period.

32. A system according to claim 31, wherein the data that is encrypted by the second computer entity is arbitrary data, said third computer entity being arranged to decrypt and return this data as evidence of its entitlement to receive the service for the current time period, and the third computer entity being arranged to respond to receipt of the correctly decrypted data from the third computer entity to provide said service to the party.

33. A system according to claim 31, wherein the data that the second computer entity is arranged to encrypt is a data component of the service.

34. A system according to claim 33, wherein the data component comprises at least one of software and digital media content.

35. A system according to claim 31, wherein the encryption key string is formed using at least an identifier of said service.

36. A system according to claim 35, wherein the third computer entity is arranged to provide said service identifier both to the first computer entity to obtain the decryption key for the service for said particular time period, and to the second computer entity.

37. A system according to claim 36, wherein the second computer entity is arranged to maps the service identifier to the most suitable one of multiple services it can provide in order to determine the service required by said party.

38. A system according to claim 35, wherein one of the first and second computer entities is arranged to generate the service identifier and to make it available both to the other of the second and first computer entities, and to the third computer entity.

39. A system according to claim 31, wherein the first computer entity is arranged to use said first means to generate plural said data sets in advance of the time periods to which they relate, the first computer entity being further arranged to make the public data of these data sets available in advance of those time periods to at least one of the second and third computer entities.

40. A system according to claim 31, wherein the time for which said service is available is divided into time slots, each said time period for which a respective said data set is arranged to be generated by said first means of the first computer entity corresponding to a respective one of said time slots.

41. A system according to claim 31, wherein the time for which said service is available is divided into time slots, at least one of said time periods for which a respective said data set is arranged to be generated by said first means of the first computer entity corresponding to a combination of multiple said time slots.

42. A system according to claim 31, wherein the time for which said service is available is divided into time slots, and wherein for a group of successive time slots, each time slot and each of every possible time-ordered combination of at least two adjacent time slots constitutes a respective said time period for which said first means of the first computer entity is arranged to generate a corresponding data set, the third means of the first computer entity being arranged to provide a single decryption key to said third computer entity upon the second means of the first computer entity determining whether the party is entitled to receive said service for any time slot or time-ordered combination of time slots within said group.

43. A system according to claim 31, wherein the first means of the first computer entity includes means for determining the occurrence of a non-clock event and for using this occurrence to start or finish of a said time period.

44. A system according to claim 31, wherein the third computer entity is a trusted platform arranged to securely store the decryption key provided to it by the first computer entity such that the decryption key is not externally accessible in cleartext form but is usable to decrypt said encrypted data in the trusted platform.

45. A computing entity according to claim 31, wherein the second means of the first computer entity is arranged to determine the entitlement of said party to any of multiple services for any of said multiple time periods, the third means of the first computer entity being arranged to provide the third computer with at least one decryption key appropriate for the or each service and the or each time period for which the party has been determined as entitled, the decryption keys for each of said multiple services in the same time period being different from each other.

46. A system according to claim 45, wherein the key-generating means of the first computer entity is arranged to use the private data of same data set for each service during the same time period when generating the decryption key to be provided to the third computer entity, the encryption key strings used for each of said multiple services being different from each other.

47. A system according to claim 45, wherein the first means of the first computer entity is arranged to generate a respective data set for each combination of service and time period, the key-generating means of the first computer entity being arranged to use the private data of the data set for the appropriate service and time period when generating the decryption key to be provided to said party.